Proof of GV bound: We shall in fact show that there exists a <u>linear</u> code that satisfies the bound above, for sufficiently large n.

To do so, we shall, as in the proof of Shannon's theorem, use a "random ensemble" of linear codes. Specifically, pick a $k \times n$ generator matrix G (with $q^k = M$), each of whose entries is picked $\sim \mathrm{Unif}(\mathbb{F}_q)$.

Note that

$$\Pr[G \text{ is full rank}] = \prod_{i=0}^{k-1} \left(\frac{q^n - q^i}{q^n}\right) = \prod_{i=0}^{k-1} (1 - q^{i-n})$$

$$\geq 1 - \sum_{i=0}^{k-1} q^{i-n}$$

$$= 1 - q^{-n}\left(\frac{q^k - 1}{q-1}\right)$$

$$\xrightarrow[n\to\infty]{} 1. \quad [\text{for } k = \alpha n,\ \alpha < 1]$$

Hence, $\exists n_0$ s.t. $\forall n \geq n_0$, G is full rank with high probability. For such a G, note that $\underline{u}G \sim \mathrm{Unif}(\mathbb{F}_q^n)$, for $\underline{u} \neq \underline{0}$, and further,

$$\Pr[\mathrm{wt}(\underline{u}G) < d \mid G \text{ full rank}] = \frac{\mathrm{Vol}(B(\underline{0}, d-1))}{q^n}.$$

Thus, via a union bound,

$$\Pr[\underbrace{\exists \underline{u} \neq \underline{0} \text{ s.t. } \mathrm{wt}(\underline{u}G) < d}_{\equiv \{d_{min}(\mathcal{C}) < d\}} \mid G \text{ full rank}] \leq q^k \cdot \frac{\mathrm{Vol}(B(\underline{0}, d-1))}{q^n}.$$

Hence, overall,

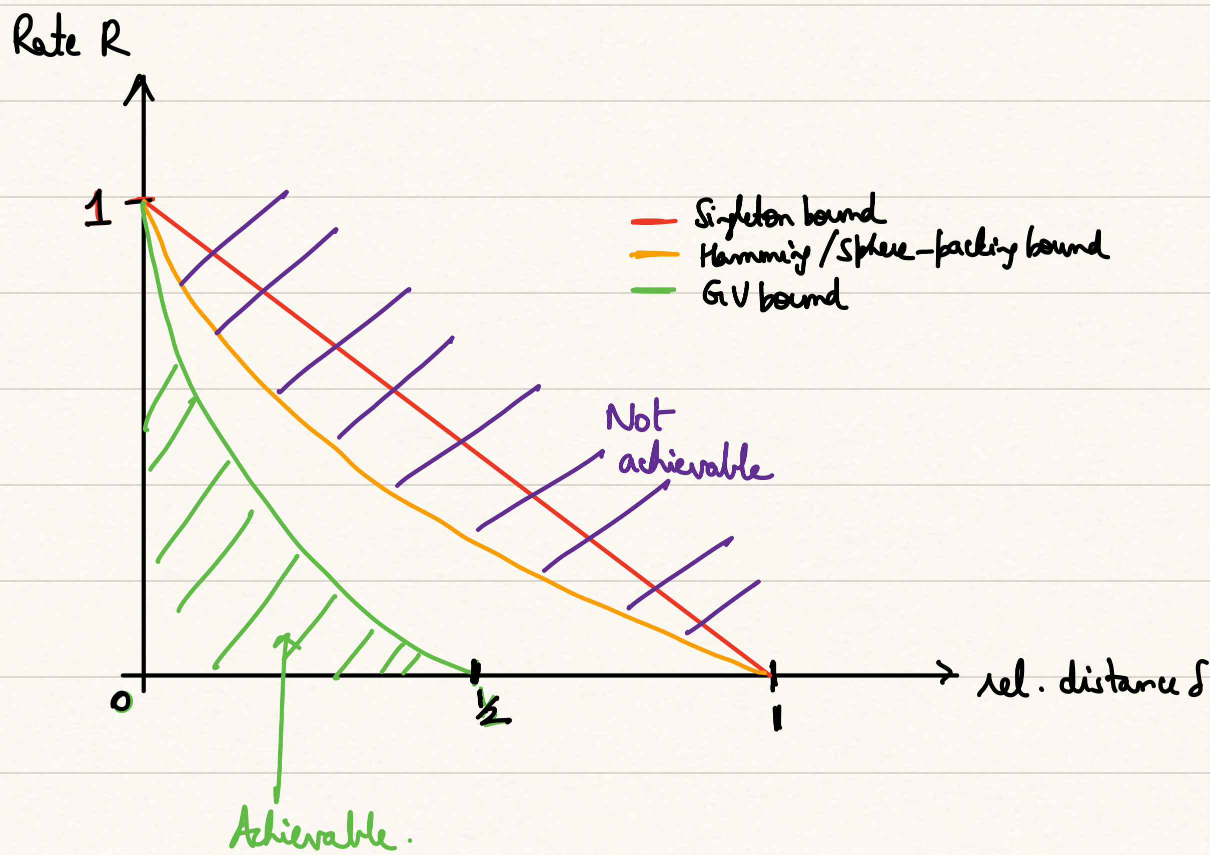
$$\Pr[\exists \text{ lin. code with } q^k \text{ codewords and min.dist.} < d]$$

$$\leq q^k \cdot \frac{\mathrm{Vol}(B(\underline{0}, d-1))}{q^n} < 1,$$

$$\text{if } \quad q^k = M \leq \frac{q^n}{\mathrm{Vol}(B(\underline{0}, d-1))} = \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}.$$

Hence, there exists a (deterministic) linear code with $M \geq \dfrac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}$. $\blacksquare$

__HW:__ Provide a different proof of the GV bound via a simple, greedy algorithm.



What is the true rate-distance tradeoff?

[Open!]

Lecture 7: More on code bounds.

Recall the bounds we had seen earlier:

(i) Hamming bound/sphere-packing bound:

$$R \leq 1 - h_q(\delta/2).$$

(ii) Singleton bound: $R \leq 1 - \delta$

(iii) GV bound: $R \gtrsim 1 - h_q(\delta)$.

A Discussion:

Fix $q=2$. Contrast these with Shannon's theorem, via the intuitive implication:

$$\underline{e} \sim (\mathrm{Ber}(p))^{\otimes n} \Rightarrow \mathrm{wt}(\underline{e}) \in \left[np - c\sqrt{n}, np + c\cdot\sqrt{n}\right], \text{w.h.p.}$$

HW: Prove the implication above, via an application of the Chebyshev inequality.

Hence, with high probability, the fraction of $\underset{\underset{\text{errors}}{|||}}{1\text{s}}$ in $\underline{e}$ is close to p, w.h.p.

Pick $\delta = \frac{d}{n} = p/2$, and consider a code $\mathcal{C}$ with relative dist. at least δ, for n suff. large. Then, via Shannon's noisy coding theorem, we have that $\mathcal{C}$ can recover from errors from a BSC(p), w.h.p., so long as the rate

$$R(\mathcal{C}) < 1 - h_b(\delta/2) \approx \text{Hamming upper bound}$$

Hence, the adversarial channel model [with exact codeword recovery] is qualitatively more stringent than the Shannon model. In what follows, we will argue that the Hamming bound can in fact NOT be attained, for suff. large δ values, in the adversarial model.

① Plotkin Bound

- The GV bound asserts the existence of codes of positive rate, if $\delta < 1/2$.
- The Hamming bound does NOT rule out codes of positive rate, for $\delta > 1/2$.

We shall show that in fact there do NOT exist codes of positive rate, if $\delta > 1/2$, in the Hamming / adversarial model [Contrast this with Shannon's theorem!]

Theorem 1: For an (n, M, d) block code over $\mathbb{F}_q$, we have

$$M \leq \frac{d}{d - \beta n}, \quad \text{for } d > \beta n,$$

where $\beta := 1 - 1/q$. [For $q = 2$, $\beta = 1/2$]

Asymptotics $(n \to \infty)$: Plotkin bound: For $\delta > \beta$, we have $R = 0$.

Proof of Thm. 1: Let $S = \sum_{\underline{u} \in \mathcal{C}} \sum_{\substack{\underline{v} \in \mathcal{C} \\ \underline{v} \neq \underline{u}}} d_H(\underline{u}, \underline{v})$.

(i) Note that $S \geq M(M-1)d$.

(ii) Now, in the following array A:

$$A = M \overbrace{\underbrace{\begin{bmatrix} \leftarrow & \underline{c}_1 & \rightarrow \\ \leftarrow & \underline{c}_2 & \rightarrow \\ & \vdots & \\ \leftarrow & \underline{c}_M & \rightarrow \end{bmatrix}}_{n}}^{\mathcal{C}} ,$$

when we pick a particular column

(a) let m_j be the # occurrences of $j \in \mathbb{F}_q$.

(b) The total # occurrences of $i \neq j$ is $M - m_j$.

Hence, the contribution of this column to S is $\sum_{j \in \mathbb{F}_q} m_j (M - m_j)$.

$$= M \cdot M - \sum_j m_j^2$$

$$= M^2 - \sum_j m_j^2 .$$

Under the constraint that $\sum_j m_j = M$, the summation $\sum_j m_j^2$ is minimized by picking $m_j = M/q$, $\forall j \in \mathbb{F}_q$. Thus, we obtain that

$$M(M-1)\, d \leq S \leq \sum_{k=1}^{n} \left(M^2 - q \left(M/q \right)^2 \right) = n M^2 \beta ,$$ yielding the statement of the theorem. ▨

The Plotkin bound can be used to obtain an improved upper bound on code sizes when $\delta < 1/2$ too. Let $q = 2$.

<u>Theorem 2</u>: For an (n, M, d) block code with $d < n/2$, we have
(Plotkin-deriv)

$$M \leq d \cdot 2^{n-2d+2}$$

Asymptotics ($n \to \infty$): For $\delta < 1/2$, we have $R \leqslant 1 - 2\delta$.

Proof of Thm. 2: Let $l = n - 2d + 1$ and let S be the first l positions $\{1, 2, \ldots, l\}$.

For each $\underline{a} \in \{0,1\}^l$, let $\mathcal{C}_a$ be the subcode of $\mathcal{C}$ consisting of codewords with $\underline{a}$ in the first l positions, projected onto S^c.

Each $\mathcal{C}_a$ is a "puncturing" of $\mathcal{C}$, with blocklength $n - l = 2d - 1$. Since $\mathcal{C}$ has min. distance d, so does each $\mathcal{C}_a$. Further, by Thm. 1, we see that since

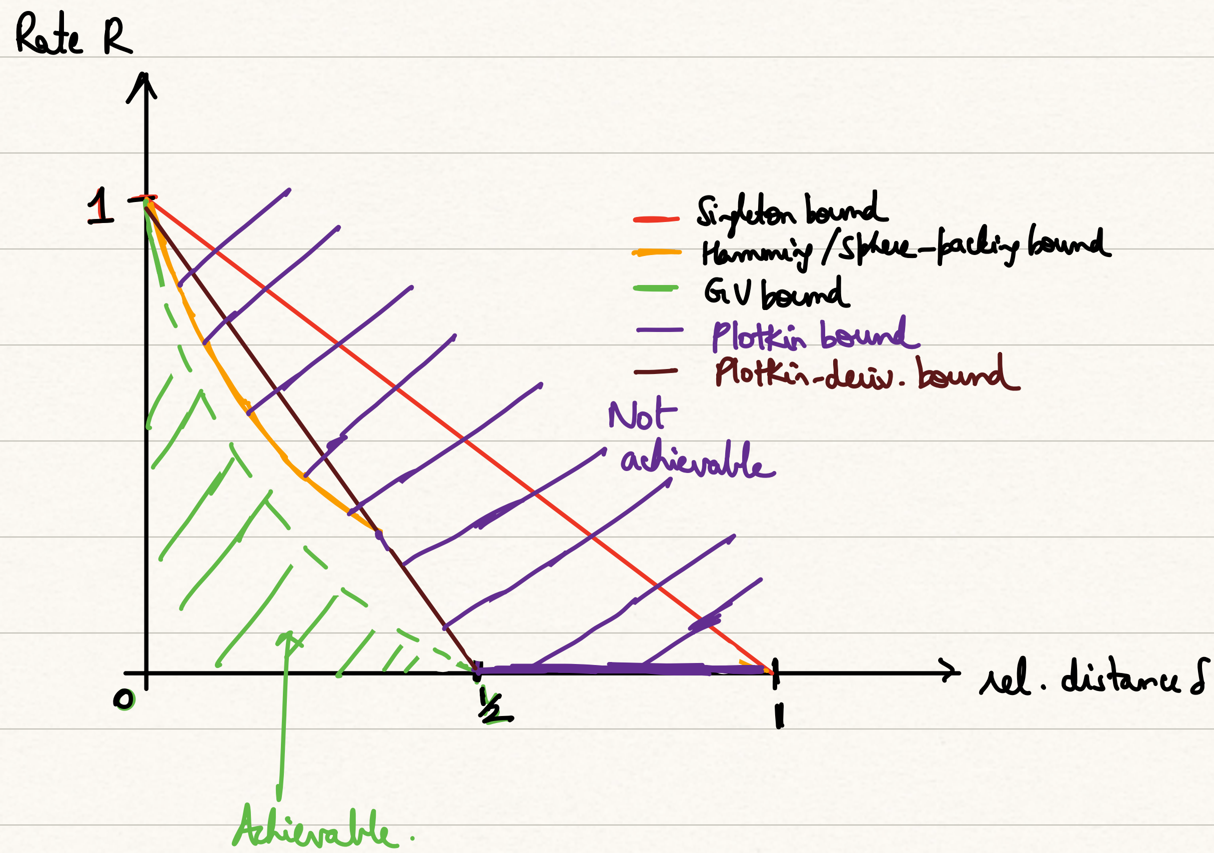
$$\frac{d_{min}(\mathcal{C}_a)}{n(\mathcal{C}_a)} = \frac{d}{2d-1} > 1/2,$$

we must have

$$|\mathcal{C}_a| \leqslant 2d.$$

Thus, since $|\mathcal{C}| = \sum_{\underline{a} \in \{0,1\}^l} |\mathcal{C}_a|$, it follows that $|\mathcal{C}| \leq d \cdot 2^{n-2d+2}$. $\blacksquare$

HW: Extend the above theorem and proof to general alphabets.



We are closing the gap b/w what is achievable & what is not...

<u>Tidbit</u>: There has been next to no improvement on the asymptotics of achievable rates over the GV bound, for the last ~ 70 years!
(G. (1952), V. (1957))

Possibly an improvement / a definitive rate-distance tradeoff will come from IIT-Madras :).

A final word on code bounds:

State-of-the-art upper bound on code sizes: MRRW bound
(McEliece, Rodemich, Rumsey, Welch (1977))

<u>Theorem 3</u> (MRRW): For binary codes, we have that

$$R \leq h_b\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right).$$

HW (reading): Read up on the Elias-Bassalygo bound.

HW: Let $A(n,d)$ and $A(n,d,w)$, respectively, be the largest sizes of an (n,M,d) binary block code and an (n,M,d) binary block code with each codeword having Hamming weight exactly w.

Prove that $A(n,d) \leq \dfrac{A(n,d,w) \cdot 2^n}{\binom{n}{w}}$.